Кожуханов Николай Михайлович
кандидат юридических наук
старший научный сотрудник
НИЛ-1 отдела исследований проблем информационной безопасности в таможенном деле
НИЦ РТА
Московская область, г. Люберцы
E-mail: 1979nic@mail.ru

Анализ проблем информационной безопасности и технической защиты информации

Для таможенных органов России стратегической целью становится информационное обеспечение процессов электронной торговли путём создания системы электронной Таможни [1]. В этой связи возрастает значение сотрудников обеспечивающих функционирование и безопасность таможенных информационных систем.

В современных условиях важнейшими элементами организации таможенного дела являются выбор оптимальной структуры таможенной службы [2] и численности её подразделений. Исследование проблем формирования состава и организационно-штатной структуры подразделений информационной безопасности и технической защиты информации таможенных органов продиктовано объективной реальностью. По данной проблеме нами было проведено исследование, результаты которого предлагаются для ознакомления и обсуждения.

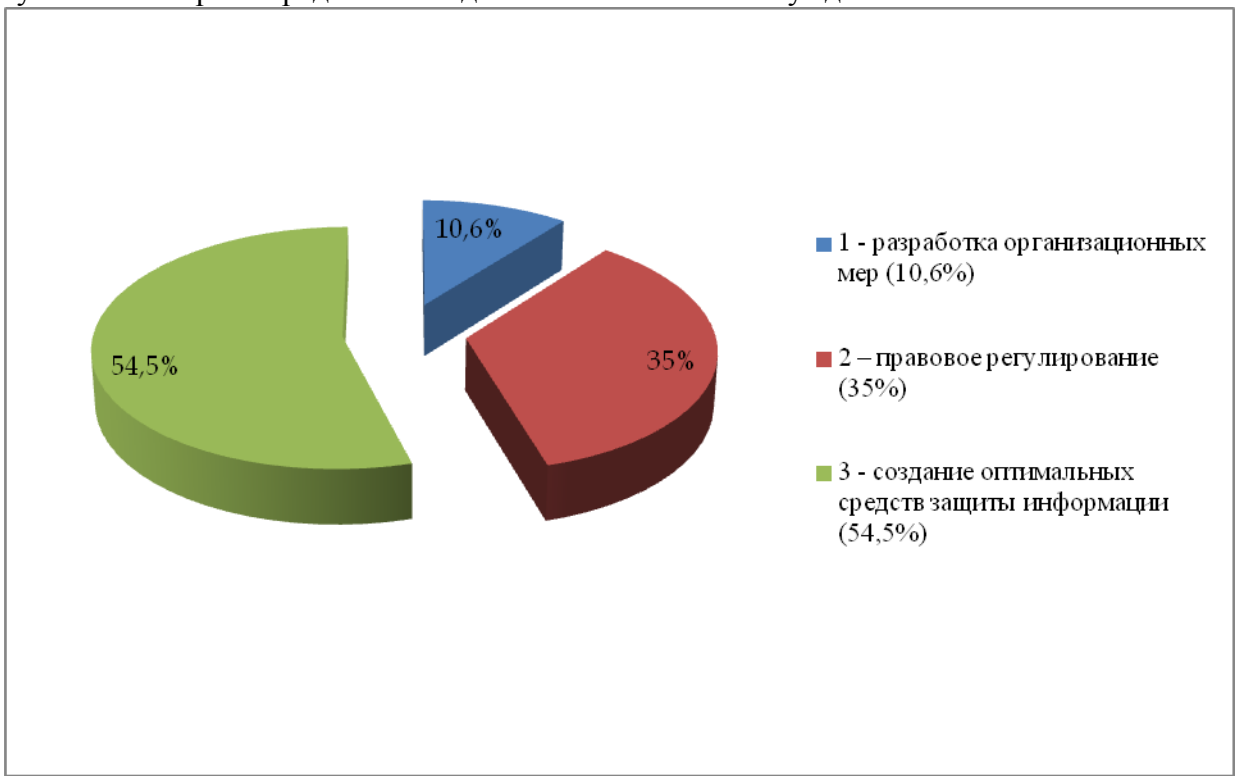

Рис. №1 Ответ респондентов на вопрос – какие из аспектов обеспечения информационной безопасности Российской федерации наиболее важны.

Большинство опрошенных – 54,5% высказали мнение, что создание оптимальных технических средств защиты информации наиболее важная сторона обеспечения информационной безопасности. Подобная позиция объективна, так как техническая защита наиболее активно применяема и с ней наиболее часто сталкиваются как работники специализированных подразделений информационной безопасности, так и неспециализированные. Техническая безопасность наиболее «наглядна». Примером могут служить антивирусные программы.

Процесс информатизации глубоко проник в таможенную сферу деятельности. Поэтому объективной необходимостью в свете высоких темпов научно-технического прогресса является и

создание современных центров обработки данных, отвечающих передовым требованиям глобализирующейся мировой торговли [3], обладающие высокой степенью технической защиты.

Правовое регулирование и организационные меры, безусловно, также имеют существенное значение в обеспечении информационной безопасности в Российской Федерации. Однако данные аспекты анализируемой проблематики можно обозначить как менее «наглядные». Так, говоря о правовом регулировании - это совокупность нормативных правовых актов, регламентирующих общественные отношения в сфере информационной безопасности таможенной деятельности Российской Федерации. Организационные аспекты информационной безопасности тесно связанны с правовыми, их сущность заключается в создание качественной организационно – штатной структуры подразделений обеспечения информационной безопасности, а также режима работы с информацией и информационными ресурсами.

Технические, правовые и организационные средства (аспекты) взаимосвязаны и образуют единую систему информационной безопасности таможенной деятельности.

Целесообразность внедрения инновационных технологий в процесс обеспечения информационной безопасности таможенного дела, на наш взгляд, обусловлена рядом взаимосвязанных факторов:

Во-первых, в развитии информационных технологий и их продвижении на мировой рынок важную роль призвана сыграть активизация инновационной деятельности, а повышение ее роли в современной экономике обусловлено тем, что в последние десятилетия произошла значительная перегруппировка факторов и источников, определяющих экономическое развитие.

По экспертным оценкам экономистов возможности экономического роста на современном этапе на 60 – 90% определяются использованием научно-технических достижений, поэтому важной составной частью государственной социально-экономической политики является инновационная политика, определяющая цели инновационной стратегии и механизма поддержки приоритетных инновационных программ и проектов.

В рамках инновационной политики Россия стоит перед необходимостью рационального вложения финансовых средств в научно-исследовательские и опытно-конструкторские работы, обеспечивающие функциональные потребности экономики страны на качественно новом уровне; развития научно-технического потенциала и повышения экономической эффективности инновационной деятельности.

Во-вторых, организация информационно-правового обеспечения защиты информации в таможенном деле, объективно предполагает внедрение в практику Таможенных органов современных информационных технологий – методов информатизации процессов и этапов управления, выполняющих функции обеспечения управленческой деятельности и, прежде всего, процесса выработки управленческих решений.

Именно информатизация управленческой деятельности способствует повышению научной обоснованности управленческих решений, приданию им таких качеств, как оперативность и своевременность их принятия, адресность, целенаправленность, наиболее полный охват позитивных и негативных факторов и т. п. «В таких условиях, – как пишет Г. В. Атаманчук, – получение новой информации, хранение и поиск уже созданной, адекватное понимание и актуальное использование информации становятся очень трудным делом, требующим времени, сил и средств, создания специальных структур (систем), применения новейшей техники и технологии» [4].

Общее понятие «информационные технологии» по своему содержанию означает систему средств и методов работы с информацией для получения информации нового качества о состоянии объекта, процесса или явления, а применительно к заявленной теме – под информационными технологиями следует понимать автоматизированную систему средств использующих определенную совокупность методов сбора, обработки (анализа), оценки и защиты социально-правовой информации в процессе выработки проектов управленческих решений.

В-третьих, информационные технологии образуют структурный элемент и составляют органическую часть более общей категории – «технология управленческой деятельности».

Как научная дисциплина технология управления исследует принципы функционирования и развития технологических систем, основные методы проектирования и внедрения новой технологии.

Эффективность использования информационных технологий определяется четкой организацией следующих этапов сбора социально-правовой информации: разработка программы действий (исследования); подбор и подготовка исполнителей; создание организационно-правовых, материально-технических и т.п. условий и творческой обстановки для их работы.

В-четвертых, в обеспечении эффективной защиты информации первичным является правовой аспект, а именно необходимость четкого разграничения информационных объектов с тем, чтобы законодательно определить правовой режим каждого из них.

Правовой режим информации как объекта правового регулирования, в первую очередь, должен рассматриваться с позиций ее доступности. Соответственно можно выделить общедоступную информацию (открытую информацию), конфиденциальную информацию (информацию ограниченного доступа) и информацию, составляющую государственную тайну (закрытую информацию).

В своей практической деятельности сотрудникам таможенных органов приходится сталкиваться со всеми указанными видами информации, однако, здесь следует обратить особое внимание вопросам защиты конфиденциальной информации в таможенном деле, которые в современных условиях становятся весьма актуальными.

При этом информационная безопасность не отождествляется только с безопасностью информации, поскольку безопасность информации является лишь компонентой, определяющей технологическую составляющую информационной безопасности.

В-пятых, возрастание прикладного значения информационных технологий в таможенном деле обусловлено расширением практики их применения в деятельности таможенных органов по противодействию угрозам защиты информационных ресурсов, связанным с использованием компьютерной техники неограниченным кругом физических и юридических лиц.

Дальнейшее повышение прикладного значения информационных технологий в таможенном деле обусловлено, с одной стороны, ростом негативных последствий глобальной информатизации, создающих внешние и внутренние угрозы национальной безопасности Российской Федерации, а, с другой, – тенденциями развития технических средств защиты информации.

В-шестых, эффективность управленческой деятельности таможенных органов зависит от многих факторов. Одним из главных является умение организовать работу с информационными ресурсами, обеспечить их надежную защиту от несанкционированного доступа.

В-седьмых, важным направлением дальнейшего развития системы таможенного администрирования, совершенствования механизмов таможенного оформления и контроля, повышения прозрачности таможенных процедур является автоматизация таможенных технологий и оперативного управления таможенной деятельностью, обеспечивающая решение следующих комплексных задач:

сбора, обработки, хранения и анализа (мониторинга) оперативной информации о состоянии процессов таможенного оформления и таможенного контроля, правоохранительной работы, других направлений деятельности таможенных органов;

планирования деятельности таможенных органов и оценки результатов (эффективности) их работы;

формирования и доведения в автоматизированном режиме до таможенных органов управляющей информации по всем направлениям их деятельности.

В-восьмых, автоматизация таможенных технологий должна сводить к минимуму негативное влияние «человеческого фактора» в принятии каждого конкретного решения путем применения информационно-технических средств, интегрированных в единую систему оперативного управления таможенной деятельностью.

Резюмируя вышеизложенное, следует отметить, что актуальность проблемы повышения прикладного значения информационных инновационных технологий в таможенном деле обусловлена возросшей диспропорцией между усилением государственно-правовых требований к

защите служебной информации, с одной стороны, и ослаблением социально-правовых мер профилактики административных правонарушений, совершаемых в сфере информации, с другой.

Возрастание прикладного значения информационных инновационных технологий в таможенном деле обусловлено расширением практики их применения в деятельности таможенных органов по противодействию угрозам, связанным с использованием компьютерной техники неограниченным кругом лиц, посягающим на защищаемые информационные ресурсы.

Дальнейшее повышение прикладного значения информационных инновационных технологий в таможенном деле обусловлено, с одной стороны, ростом негативных последствий глобальной информатизации, создающих внешние и внутренние угрозы национальной безопасности Российской Федерации, а, с другой стороны, тенденциями развития технических средств защиты информации.

Эффективность управленческой деятельности таможенных органов зависит от множества факторов. Одним из основных является умение организовать работу с информационными ресурсами, обеспечить их надёжную защиту от несанкционированного доступа.

Автоматизация таможенных технологий должна сводиться к минимальному влиянию «человеческого фактора» на принятие каждого конкретного решения путём применения информационно – технических средств, интегрированных в единую систему оперативного управления таможенной деятельностью. В этом свете возникает необходимость подготовки специалистов разносторонне подготовленных, которые будут одинаково профессиональны на техническом, правовом и организационном поле деятельности.

«Вес» угроз может определяться не только степенью их распространения, но и спецификой пространства, на котором они проявляются [5]. В вопросе – «как респонденты оценивают состояние правового обеспечения информационной безопасности в таможенной сфере деятельности», анализировались угрозы связанные с возможностью заложения в нормативные правовые акты «брешей» в модели обеспечения информационной безопасности, с наличием пробелов права и закона, с противоречиями между различными правовыми регуляторами, которые влекут за собой нарушение режима безопасности информации.

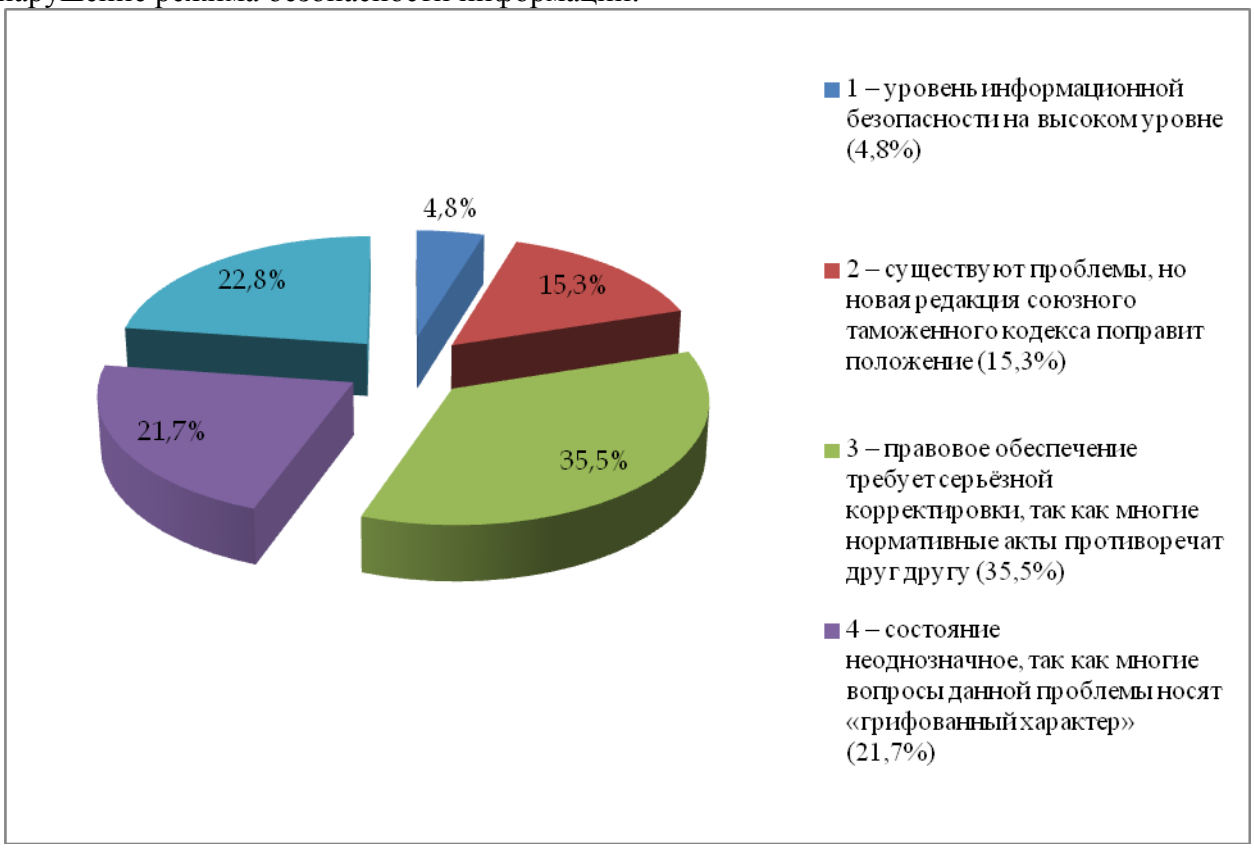

Рисунок №2 Ответ респондентов на вопрос - как ими оценивается состояние правового обеспечения информационной безопасности в таможенной сфере деятельности

Большинство респондентов – 35,5%, высказали мнение, что правовое обеспечение информационной безопасности в таможенной сфере деятельности требует серьёзно корректировки, так как многие нормативные акты противоречат друг другу.

На наш взгляд, особого внимания требует приведение существующей правовой базы к единой логике. Необходима оптимизация существующих правовых режимов информационной безопасности. Требуется чёткое закрепление принципов, на которых будет построен алгоритм принятия управленческих решений, позволяющий максимально эффективно обеспечить информационную безопасность в таможенной сфере деятельности.

В качестве основополагающих принципов, которыми следует руководствоваться в обеспечении информационной безопасности таможенной деятельности являются: 1) невозможность миновать защитные средства; 2) усиление самого слабого звена; 3) недопустимость перехода в открытое состояние; 4) минимизация привилегий; 5) разделение обязанностей; 6) многоуровневая защита; 7) разнообразие защитных средств; 8) простота и управляемость информационной системы; 9) обеспечение всеобщей поддержки мет безопасности.

1. Принцип невозможности миновать защитные средства означает, что все информационные потоки в защищаемую сеть и из неё должны проходить через систему защиты информации.

2. Надёжность любой системы защиты информации определяется самым слабым звеном. Часто таким звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения информационной безопасности приобретает нетехнический характер.

3. Принцип недопустимости перехода в открытое состояние означает, что при любых обстоятельствах (в том числе нештатных), средства защиты информации полностью выполняет свои функции, либо должна полностью блокировать доступ.

4. Принцип минимизации привилегий предписывает выделять пользователям и администраторам только те права на доступ, которые необходимы им для выполнения служебных обязанностей.

5. Принцип разделения обязанностей предполагает такое распределение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс. Это особенно важно для предотвращения злонамеренных или неквалифицированных действий системного администратора.

6. Принцип многоуровневой защиты предписывает не полагаться на один защитный рубеж, каким бы надёжным он ни оказался. За средствами физической защиты должны следовать программно-технические средства, за идентификацией и аутентификацией – управление доступом и, как последний рубеж, - протоколирование и аудит. Эшелонированная оборона способна по крайней мере задержать злоумышленника, а наличие такого рубежа, как протоколирование и аудит, существенно затрудняет незаметное выполнение злоумышленных действий.

7. Принцип разнообразия защитных средств рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками преодоления средств защиты информации.

8. Принцип простоты и управляемости системы в целом и средствами защиты информации в особенности определяет возможность формального или неформального доказательства корректности реализации механизмов защиты. Только в простой и управляемой системе можно проверить согласованность конфигурации разных компонентов и осуществить централизованное администрирование.

9. Принцип всеобщей поддержки мер безопасности носит нетехнический характер. Рекомендуется с самого начала предусмотреть комплекс мер, направленный на обеспечение лояльности персонала, на постоянное обучение, теоретическое и, главное, практическое.

Анализирую современное устройство обеспечения иформационной безопсности и проводя предварительное интервьюирование, которое предществовало проведению опроса, нами была выявленна проблема излишней формальной бюрократизированности процесса обеспечения информационной безопасности. За обилием регламентов и предписаний страдает качество

производимых операций по обеспечению информационной безопасности таможенной деятельности. Опрос подтвердил этот факт. 46,6% респондетов подтвердили данное явление.

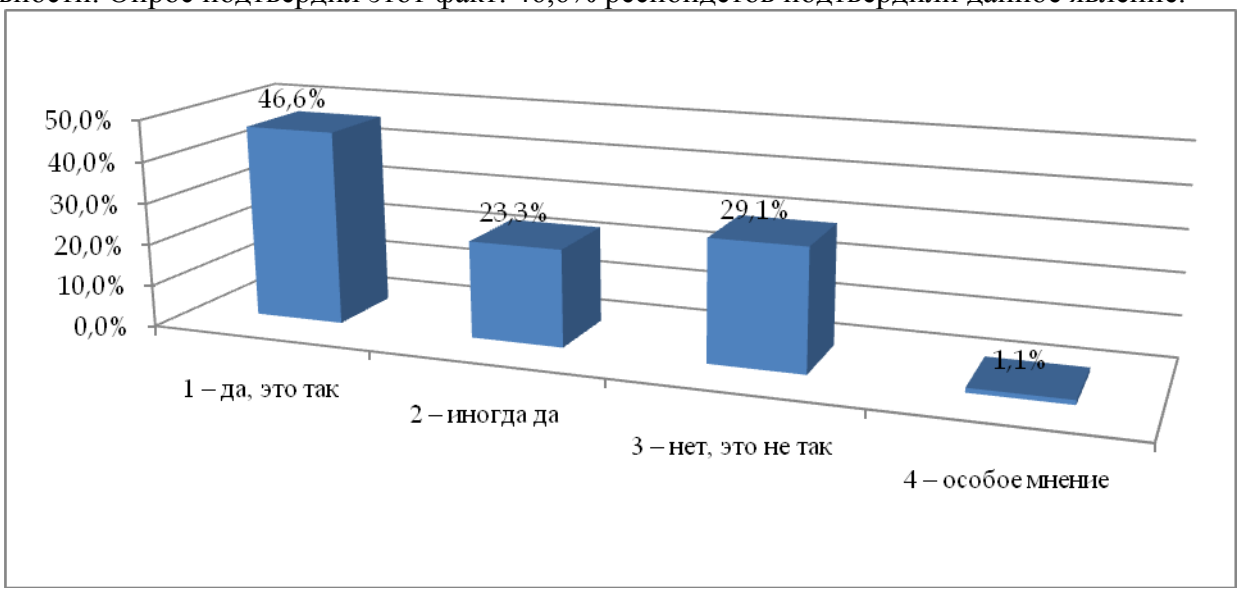

Рисунок №3 Ответ респондентов на вопрос – не считаете ли вы, что процесс организации обеспечения информационной безопасности сводится к формальным бюрократическим условностям, которые реально не влияют на состояние защищенности

Таможенные органы, получая сведения различного качества конфиденциальности подходят к данной информации как к информации ограниченного доступа, за исключение сведений носящих сопровождающий, консультативный характер, то есть относящихся к категории общедоступной информации. 63% респондентов подтвердили данную позицию.

С другой стороны таможенные органы оперируют информацией, которая в соответствии с федеральными законами подлежит предоставлению, то есть её получение это часть регламента прохождения таможенных процедур.

Анализ, основанный на материалах проведённого нами опроса, позволяет говорить об актуальности исследования проблем формирования состава и организационно-штатной структуры подразделений информационной безопасности и технической защиты информации таможенных органов. Своевременность данного исследования продиктована не только управленческими решениями ФТС России, но и объективными закономерностями. Так, информатизация таможенных процессов требует привлечения высококвалифицированных специалистов техников, которые смогли бы всесторонне обеспечивать все информационные операции. Таможенные информационные технологии становятся все более совершенными в техническом смысле и требуют большего внимания в обслуживании, что требует увеличить штатную численность специалистов обеспечивающих их функционирование и защиту.

К ещё одному ключевому аргументу увеличения числа специалистов подразделений информационной безопасности и технической защиты информации таможенных органов выступает тот факт, что современная таможня просто не сможет приносить установившейся в настоящее время уровень отчислений в казну, которые формируют доходную часть бюджета России, и тем более наращивать темпы внешней торговли, не используя информационные технологии и не модернизируя их. Стоит, в результате хакерской атаки, «зависнуть» информационной системе отдельной взятой таможни и это вызовет фактически полный коллапс в её работе. Создаётся прямая угроза экономической безопасности государства.

С другой стороны, увеличивая количество специалистов подразделений информационной безопасности и технической защиты информации таможенных органов нельзя забывать о необходимости повышения их профессиональных навыков.

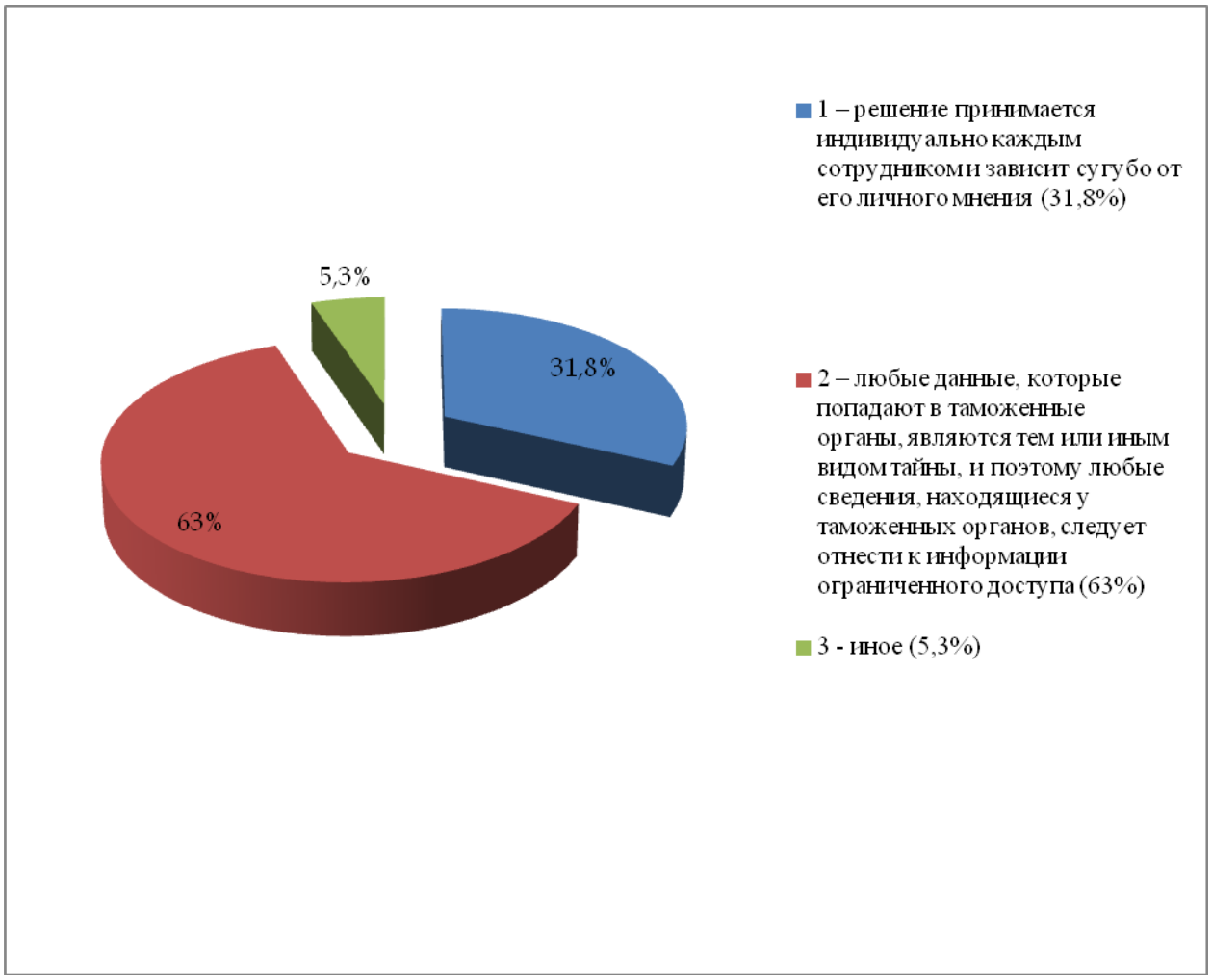

Рисунок №4 Ответ респондентов на вопрос – каким образом сотрудники таможенных органов определяют, к какому виду информации ограниченного доступа относятся данные, которыми они оперируют

Динамика развития правового регулирования таможенной сферы общественных отношений, выдвигает новые требования к самим специалистам осуществляющим техническое обслуживание. Их уровень умений, знаний и навыков должен выходить за рамки их узкой специализации. Необходимо не только техническое обеспечение, но и организационно – правовой контроль всех информационных процессов проходимых на таможне, что требует повысить уровень знаний нормативных правовых актов, регламентирующих таможенную деятельность как вид государственной деятельности.

Резюмируя вышеизложенное скажем, что к наиболее важным проблемам обеспечения информационной безопасности в таможенных органах относятся:

- недостаточная штатная численность подразделений информационной безопасности, с учётом функций и задач, а также территориального расположения отдельных объектов обеспечения;
- потребность в повышении юридической квалификации персонала таможенных органов;
- необходимость создания в рамках Комиссии Таможенного Союза специализированного подразделения, целью которого будет решение правовых, организационных и технических вопросов обеспечения информационной безопасности таможенной деятельности.

1. Шашаев А.Е. Перспективные направления долгосрочного развития информационно-технического обеспечения Федеральной таможенной службы / сборник материалов международной научно-практической конференции 7-8 апреля 2011года «Единое окно», об-

мен данными, межведомственное и государственно-частное сотрудничество при упрощении процедур торговли. – М. 2011 С.229.
2. Маколова Л.В. оптимизация численности персонала с учётом результативности работы / материалы научно-практического семинара Оптимизация таможенных процедур: от поиска решений к их реализации. – Ростов-на-Дону. 2009. С.51.
3. Слынько Е.Н. Информация – основа таможенной разведки / Вестник РТА. – М. 2009. №4. С. 86.
4. Атаманчук Г. В. Государственное управление. - М. 1997. С. 240.
5. Терновая Л.О. Внешние и внутренние угрозы безопасности: проблемы измерения / Вестник РТА. – М. 2009. №2. С.72.